Royal College of General Practitioners (RCGP) organisational response to NHS England's consultation on the national review of clinical risk management standards DCB0129 and DCB0160

September 2026

About RCGP

We are the professional membership body for GPs in the UK. Our purpose is to encourage, foster and maintain the highest possible standards in general medical practice. We support GPs through all stages of their career, from medical students considering general practice, through to training, qualified years and retirement.

National review of clinical risk management standards DCB0129 and DCB0160

NHS England

These mandatory standards protect patients by ensuring all health IT systems (for example, electronic patient records and clinical decision support systems) are properly assessed for clinical risks before they are used in patient care. DCB0129 sets out requirements for technology manufacturers and DCB0160 covers how health and social care organisations deploy and use these systems safely.

NHS England is reviewing these standards to reflect advances in healthcare technology. For example, artificial intelligence supporting clinical decisions, complex interconnected systems sharing data across organisations, and new technologies like voice recognition and machine learning becoming routine in patient care.

Consultation questions

Scope of the standards

5. Should alternative risk management standards be adopted in health and adult social care in place of the current standards?

- **Yes (please suggest an alternative)**
- **No**
- **Don't know**

DCB0129 and DCB0160 provide an important framework for managing clinical risk from health IT and should be modernised rather than replaced.

The review should address areas where the existing standards do not sufficiently reflect how digital technologies are now developed, deployed and used. They should better address technologies operating across organisational and system boundaries, rapidly changing technologies such as AI, ongoing risk management after deployment, and how safety information and learning are shared between manufacturers, deploying organisations and the wider health system.

Implementation guidance will also be important in translating the standards into workable clinical-safety arrangements, particularly for smaller organisations and where responsibility for procurement, infrastructure, deployment and specialist clinical-safety support is distributed across different organisations.

6. Do you think that DCB0129 and DCB0160 should apply to medical devices?

- **Yes**
- **No**
- **Don't know**

Where a medical device is also a product used to provide electronic information for health or social care purposes, DCB0129 and DCB0160 should continue to apply to the clinical risks arising from its development, deployment and use within health and care systems.

The standards should complement, rather than duplicate, medical-device regulation. DCB0129 and DCB0160 are particularly important in addressing risks arising from local configuration, integration with other systems, clinical workflow and use within a particular care setting, which may not be fully addressed through regulation of the device itself.

Equally, the standards must continue to apply to health IT that is not regulated as a medical device. Significant clinical risk can arise from technologies outside the medical-device framework, including systems that communicate, summarise, transfer or present clinical information.

7. Do you think that the standards should include specific cybersecurity requirements for health IT systems?

- **Yes**
- **No**
- **Don't know**

It is critical that cybersecurity is robustly safeguarded for all health IT systems. While there are other cybersecurity requirements for manufacturers and deployers, such as the Digital Technology Assessment Criteria (DTAC) and the Data Security and Protection Toolkit

(DSPT) respectively, the RCGP has not gathered enough evidence to state that they are sufficient for managing risk in health IT systems. This should be carefully considered and additional cybersecurity requirements implemented if existing tools are not sufficient.

Terminology

8. Are there specific definitions or terms within the current standards that require further clarification or updating?

- **Yes**
- **No**
- **Don't know**

The standards should better define how responsibilities apply where deployment, procurement, infrastructure, configuration and specialist clinical-safety support sit across different organisations.

They should distinguish between the organisation responsible for managing clinical risk and another organisation providing specialist expertise or carrying out elements of the assurance process on its behalf.

Greater clarity would also be helpful where a risk or control crosses organisational boundaries, including where the deploying organisation identifies a hazard but does not have the authority or capability to control its underlying cause.

9. The word 'clinical' is used extensively in the standards to contextualise risk management and digital clinical safety. Do you think the word should remain or be replaced?

- **Remain**
- **Be replaced (please suggest an alternative)**
- **Don't know**

The term “clinical safety” remains useful because it describes the particular expertise and methods used to understand risks to patient care arising from health technology.

However, digital clinical safety should sit clearly within the wider patient-safety system rather than operate as a separate discipline. Patient-safety reporting and learning processes should be able to identify when digital technology has contributed to an incident and ensure that those concerns can be reviewed, aggregated and escalated appropriately.

Risk-based classification and tiered approaches

10. Should the standards include different requirements based on the risk profile of the technology? (for example, a smaller subset of requirements is applicable to lower risk products)?

- **Yes**
- **No**
- **Don't know**

The requirements should be proportionate to the level of risk. A core set of requirements should apply to all health IT, with additional assurance for higher-risk technologies.

The initial risk category should be based on what the technology is being used to do in clinical care and the potential consequences if it goes wrong. A technically simple component may still require a high level of assurance if it affects diagnosis, prescribing, treatment, eligibility for care or other important clinical decisions, particularly where it is used at scale.

Higher-risk technologies may require more extensive testing, stronger change control and closer monitoring after deployment.

Clinical safety officers (CSOs)

11. Should the requirement for a CSO remain in the standards?

- **Yes**
- **No**
- **Don't know**

The CSO role provides important clinical expertise and leadership in identifying and managing risks arising from health IT, and the requirement should remain.

For smaller organisations such as general practices, this does not necessarily mean employing a CSO within each organisation. Shared or externally provided CSO support can be appropriate, provided the deploying organisation, such as a general practice, retains responsibility for clinical risk management under DCB0160 and is satisfied that the support it relies on is competent and appropriate.

12. Does the CSO role need further definition?

- **Yes**
- **No**
- **Don't know**

The role should be clearer about the responsibilities of the CSO within the clinical risk management process, particularly where CSO support is shared or provided by another organisation.

The standards should make clear that the CSO provides clinical-safety expertise and oversight but does not take responsibility for clinical risk management away from the deploying organisation. They should also clarify the CSO's role and the routes available for escalating hazards where the action needed to control the risk sits outside that organisation, for example with a supplier, commissioner, national system owner or another provider.

13. Do you think the standards should include a defined supporting role to the CSO and clearer responsibilities for related roles?

- **Yes**
- **No**
- **Don't know**

Clinical safety is multidisciplinary, and the standards should more clearly define the responsibilities of those who support the CSO, including technical, cybersecurity, patient-safety, human-factors and information-governance expertise where relevant.

For smaller organisations, some of this expertise may be accessed through shared or external services rather than provided internally.

Documentation and development practices

14. Do the mandated safety deliverables need revision in any way?

- **Yes**
- **No**
- **Don't know**

The mandated safety deliverables should make it easier to identify and trace clinical risks that span organisational and system boundaries.

The current approach already allows controls to be transferred between organisations, but where a hazard depends on multiple systems or organisations it can be difficult to maintain a clear end-to-end view of the risk. The documentation should therefore make explicit where responsibility for controls sits, what dependencies exist on other organisations or systems, and whether transferred controls have been accepted and addressed.

It would also be helpful for related hazards and controls to be traceable across the safety documentation maintained by manufacturers, national system owners and deploying organisations.

15. Should the standards accommodate modern development and deployment lifecycle practices (for example, agile methodologies)?

- **Yes**

- **No**
- **Don't know**

The standards should support modern development approaches where systems are updated iteratively rather than through occasional major releases.

Clinical safety activity should therefore be able to continue alongside development, with proportionate reassessment when changes could affect clinical risk. The standards should focus on maintaining effective clinical risk management and an auditable record of decisions, rather than requiring a fixed documentation process that is difficult to keep aligned with frequent changes.

16. Are all phases of a product lifecycle sufficiently addressed by the standards?

- **Yes**
- **No**
- **Don't know**

The standards should place greater emphasis on clinical risk management after initial deployment. Risk can change as software is updated, configurations change, systems are integrated differently, or new hazards emerge through routine use.

There should be clear expectations for ongoing monitoring, review of incidents and near misses, reassessment following material changes, and incorporation of new safety information into the safety case and hazard log. Where learning identifies risks that may affect other organisations using the same technology or pathway, there should also be a route for that learning to be shared with manufacturers, system owners and other deploying organisations.

The standards should also support the systematic capture and reuse of safety learning generated before wider deployment, including learning from controlled testing and regulatory sandbox activity. This may be particularly important for technologies that fall outside medical device regulation, where there may otherwise be fewer mechanisms for safety learning to be accumulated and shared.

Decommissioning should also be treated as a clinical safety issue where removal or replacement of a system could affect continuity of care, access to information or established workflows.

Patient safety

20. How could the standards and/or implementation guidance be better aligned to the broader effort to improve patient safety? Please also consider the role of clinical safety officers (CSOs).

Digital clinical safety should be more clearly integrated with wider patient-safety reporting and learning.

Staff should be able to identify when digital technology may have contributed to an incident, regardless of the main type of incident. Reporting mechanisms should be simple, well signposted and connected with existing patient-safety systems, with appropriate routes for specialist clinical-safety review and escalation.

CSOs should have clear routes to escalate concerns where the action needed to control a risk sits outside their organisation. Learning should also be capable of being aggregated and shared across organisations where the same technology, supplier or underlying hazard is involved.

For example, consideration could be given to whether national patient-safety reporting arrangements could support a more systematic view of digital clinical-safety incidents and hazards, so that recurring problems can be identified and learning shared across the system.

Sector-specific implementation

33. What are the key sector-specific challenges that need to be addressed in the implementation guidance?

General practice differs from larger provider organisations because responsibility for digital systems is often distributed across practices, ICBs, NHS England and suppliers. A practice may be responsible for local deployment and use while relying on other organisations for procurement, infrastructure, configuration and specialist clinical-safety support.

Implementation guidance should reflect this explicitly. It should clarify how responsibilities operate at these organisational boundaries, particularly where a practice identifies a risk but does not have the authority or capability to control its underlying cause.

Where clinical-safety expertise, including CSO support, is provided outside the practice, there is an additional need to ensure that safety information arising from day-to-day clinical use reaches those responsible for the clinical risk-management process. Incidents, near misses, changes in workflow and newly identified hazards should be capable of informing the hazard log and clinical safety case, while relevant safety learning and changes in controls should be communicated back to the practice. Guidance should make clear how these interfaces should operate while preserving clear responsibility for local deployment and use.

The Pharmacy First implementation through GP Connect Update Record provides a practical example: the information model, national transfer mechanism, pharmacy systems

and receiving GP systems sat across different organisations, making it difficult to identify where responsibility lay for assuring the end-to-end clinical risk.

Recent HSSIB work on e-RS found variation in how DCB0160 responsibilities were understood in general practice, including uncertainty about whether responsibility sat with practices, PCNs or ICBs, and limitations in ICB capacity and capability to provide support.

34. How could the implementation guidance better support smaller health and care organisations with limited resources, whilst maintaining safety requirements?

Implementation guidance should provide a practical model for how smaller organisations can discharge their clinical-safety responsibilities while drawing on shared specialist expertise.

In general practice, this should include clear guidance on the roles and boundaries where CSO support is provided by an ICB or another shared service. It should be clear what remains the responsibility of the practice, what the shared CSO service is expected to do, who maintains and updates the relevant clinical safety documentation, how practices contribute local knowledge and experience, and how risks are escalated where neither the practice nor the shared CSO service has the authority to control the underlying cause.

The guidance should also describe how information should flow between the practice and the shared clinical-safety function. Hazards, incidents, near misses, changes in workflow and local exceptions identified through routine clinical use should be capable of informing the wider clinical risk-management process. Equally, practices should receive feedback about resulting changes in controls, supplier action or other safety learning. This is particularly important if the CSO is not embedded within the organisation using the technology day to day.

Implementation guidance should also describe models for peer learning between smaller organisations. As is being implemented in some local areas, this could include a GP Federation developing a community of practice of trained GP practice CSOs, or ICBs hosting regular digital clinical safety meetings through which incidents and learning can be discussed and disseminated. Such arrangements could provide a route for problems identified in one practice to be shared with others, recurring hazards to be recognised, and concerns requiring action at supplier or system level to be escalated.

Smaller organisations can retain responsibility for clinical risk management within their own deployment and use of technology, while also contributing to wider system-level safety learning. Practices should be able to identify and manage hazards arising from local clinical workflows, report incidents and near misses, assess whether proposed controls are effective in their context, participate in joint hazard reviews where appropriate, and ensure that new risks and learning are escalated and shared beyond the practice when they may affect other organisations.

However, guidance alone will not resolve the problems if the specialist capability it assumes is not available. Recent HSSIB work on e-RS found uncertainty about how DCB0160 responsibilities operated between practices, PCNs and ICBs and limitations in ICB capacity and capability to provide clinical safety support.

Smaller organisations therefore need reliable access to adequately and recurrently funded clinical-safety expertise; this should not depend on whether an individual ICB happens to retain sufficient digital or clinical safety capacity.

This is particularly important if revised standards are to use the enhanced statutory powers introduced since the current versions were published. The existing DCB0160 was developed when organisations were required to "have regard to" information standards; NHS England's consultation confirms that this remains the position for the current standard, but that future revisions are likely to use the newer powers. Before requirements become more prescriptive, the implementation model for general practice needs to be clear, workable and supported by the necessary infrastructure and appropriate resourcing.

35. How can the standards be more effectively applied across systems (for example, where similar technology may be deployed across multiple organisations)?

The standards should better support clinical risk management across multiple organisations using the same technology or participating in the same digital pathway.

Where appropriate, manufacturers, national system owners, commissioners and deploying organisations should be able to contribute to shared hazard identification and system-level clinical-safety activity, rather than each organisation independently identifying the same hazards. Known hazards, relevant controls and safety learning should be capable of being shared across deployments.

Where a hazard identified locally arises from a supplier product or another part of a cross-organisational digital pathway, there should be a clear mechanism for escalating it to the organisation able to address the underlying cause and for sharing the resulting learning with other organisations using the same technology or pathway.

As set out above, the Pharmacy First implementation through GP Connect Update Record illustrates the need for this approach. The information model, national transfer mechanism, pharmacy systems and receiving GP systems sat across different organisations. Effective clinical risk management therefore requires both local assurance and a means of understanding and managing risks across the end-to-end pathway.

NHS England and DHSC should therefore ensure that there is a nationally funded clinical-safety capability for widely deployed health IT. This should be able to undertake or coordinate reusable hazard analysis, testing and, where appropriate, quantitative evaluation; maintain shared safety evidence; develop assurance blueprints covering common deployment models; and aggregate post-deployment safety information across organisations. Regional or ICB services may contribute to delivery, but access to this

capability should be nationally assured rather than dependent on local organisational capacity.

This national or shared assurance should support, rather than replace, the deploying organisation's responsibilities under DCB0160. Practices should remain responsible for assessing how a technology operates within their own configuration, workflow, workforce, interfaces and patient population, implementing appropriate local controls and accepting the residual risks that they genuinely control. The purpose of shared assurance is to prevent thousands of smaller organisations repeatedly attempting specialist assessments that can be undertaken more rigorously once at the appropriate level.